Information Assurance @ Goddard

A SQL Injection Story

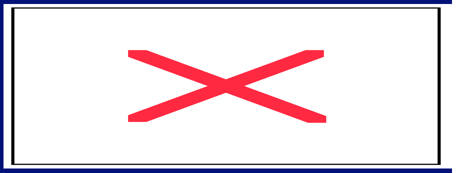
Panelists

- Ron Colvin – Moderator
- Michael Stone – Incident Response
- Joel Offenberg – CSO
- Dennis Fitzgerald – NGIN Developer
- Bill Mecca – System Administrator
- Andy Gravatt – Software Manager

Compromise –Vulnerability

- SQL Injection on login page
  - –SELECT statement used “username” without validation
- Errors sent to web client
- MS SQL xp's enabled
- SQL server running with sufficient privilege to write to web directory

Compromise – Exploit



- Attackers sent SQL via login username
- Retrieved usernames & passwords
- Installed backdoor
- More than half a dozen IPs involved
  - Various foreign addresses
  - Intruders contacted other systems on the network searching for additional targets

Compromise – Response

- Contact sysadmin for access to system
- Contact CSO & other security personnel
- Find web admin or developer for information about the web application
- Interviews to understand system
- Conduct console review & begin forensic analysis

CSO – Notification

- Prior to this incident, one of the admins asked for the incident response form for a possible incident on another system.
- IRT contacts sys admin or me?
- CNE Block Notification posted Mon, 18 Jul 2005 10:19:43

CSO – Response

- 18 July (Monday) CSO notifies system admin, Crime Scene banner delivered, instructed not to touch
  - IRT preliminary visit (?)
- 19 July Sys Admin issues e-mail notice to user community of "Unscheduled NGIN Maintenance" of uncertain duration
- 20 July IRT imaged the disk and returned it to owner, releases for rebuilding
  - Rebuild system & install service pack 1 for Microsoft Server 2003
  - send to Sys Admin incident form, reminder to complete
  - Forward Krage recommendation to use owasp.org site
- 21 July Initially heard intrusion via port 446 (?)
  - Incident report submitted
  - Update IPAMS to correct OS from Win2000 to Server 2003
- 22 July ITCD/CITSM issues IT Security Alert for NGIN
  - Steve Padgett issues login patch procedure
  - Code 400 DCSE sends PKI message with some details
- 25 July Certification Scan requested #2144, results in 1 Med vuln (false pos?)
- 27 July Certification Scan requested #2152, results in 4 Med vuln!
- 28 July Passed ISS scan #2155, unblock request sent to DCSO

CSO – Lessons Learned

- Ensure sys admins have incident forms, evidence banner, and procedure for use
- Keep a log of incident activity

Developer – Response

- Researched attack on web
- Identified main risk: the Login script
- Modified script to validate user input
  - Disallow characters that can’t occur in a username
  - Password was already checked in script, not in SQL
- Published fix to NGIN community

Developer – Methods for Future

- Validate all user inputs on server
  - Don’t rely on form or javascript to validate
- Switch to parameterized queries and commands instead of building SQL in script
  - Encourage Macromedia to do likewise
- Logging
  - Improve data logged
  - Build analysis tools
  - Review logs regularly

Sys Admin -- Notification

- July 22nd an email from Hank Middleton to DCSOs and DCSEs regarding NGIN
- I notified Bill Mecca (Admin) and the CSO
- Patch available for download

Sys Admin -- Response

- Attempted to patch system with new login page
- 550 system incompatible with JWST patch
- Tried to compare notes with other NGIN Admins and POCs
- System was taken offline until patch was ready

Sys Admin – Lessons Learned

- Better safe than sorry, take it off-line if possible
- Where Custom Code and requirements are the priorities canned solutions may not work
- Configuration Management of the Application itself was needed
- Additional firewall where user base is known

Software Best Practices

- Code Reviews
- Independent developer attack
  - Have outside developer attempt to break into site
  - Even better if you let him/her see the code
- Coding Practices
  - Validate the input lengths
  - Validate that the input matches the data type expected (Number, String, etc.)
  - If input is a string, escape the single quotes (change single quote to two single quotes)
  - Look for special characters that don’t need to be in the input (<, >, @, ;, etc)
  - Use parameterized database calls
    - ColdFusion – cfqueryparam
    - Java, VB, Perl, PHP – prepared statements

Additional Information

- Web sites:
  - http://www.owasp.org/ - Open Web Application Security Project
  - https://buildsecurityin.us-cert.gov/portal - DHS security site
  - http://webmaster.gsfc.nasa.gov/security - GSFC's security site
  - http://developers.sun.com/learning/javaoneonline/2005/webtier/TS-5935.pdf - JavaOne presentation on hacking websites

Discussion